TU Verkündungsblatt
Amtliche Bekanntmachungen

Herausgegeben vom
Präsidenten der
Technischen Universität
Carolo-Wilhelmina
zu Braunschweig

Redaktion:
TU-Abteilung 36
Pockelsstraße 14
38106 Braunschweig
Tel. 0531/391-4308
Fax 0531/391-4575

An die Dienststellen
gemäß Verteiler TU 3

Abteilung 36 (20 Ex)

Aushang

Nr. 272
07.07.2003

Ordnung zur IT-Sicherheit der Technischen Universität Braunschweig

Der Senat der Technischen Universität Braunschweig hat in seiner Sitzung am 04.06.2003 die o.g. Ordnung zur IT-Sicherheit der Technischen Universität Braunschweig beschlossen, die hiermit hochschulöffentlich bekanntgemacht wird.

Die Ordnung tritt am Tage nach ihrer hochschulöffentlichen Bekanntmachung, am 08.07.2003, in Kraft.

Ordnung zur IT-Sicherheit der Technischen Universität Braunschweig

Inhaltsverzeichnis

Präambel

Ein leistungsfähiger Universitätsbetrieb erfordert in zunehmendem Maß die Integration von Verfahren und Abläufen, die sich auf Informationstechnik (IT) und hierbei insbesondere auf vernetzte IT-Systeme stützen. Dafür ist die Sicherstellung der Integrität, Vertraulichkeit und Verfügbarkeit von Daten, Programmen und Diensten zwingend erforderlich. Insbesondere die Anbindung der IT-Systeme an das weltweite Datennetz erfordert wirksamen Schutz gegen Fremdeingriffe. Die Thematik der "Sicherheit in der Informationstechnik" ("IT-Sicherheit") bekommt damit für die Technische Universität Braunschweig eine grundsätzliche Bedeutung, die die Entwicklung und Umsetzung eines einheitlichen Sicherheitskonzepts für die Universität erforderlich macht.

§ 1
Gegenstand dieser Ordnung

Gegenstand dieser Ordnung ist die Festlegung der zur Realisierung eines universitätsweiten IT-Sicherheitsprozesses erforderlichen Verantwortungsstrukturen unter Berücksichtigung der einschlägigen gesetzlichen Bestimmungen, der Informationsdienste-Ordnung sowie der Nutzungsordnung zur Informationstechnologie.

§ 2
Geltungsbereich

Der Geltungsbereich dieser Ordnung erstreckt sich auf alle Einrichtungen der Technischen Universität (Fachbereiche, wissenschaftliche Einrichtungen, Einrichtungen mit zentraler Funktion, sonstige Einrichtungen) und in technischer Hinsicht auf die gesamte IT-Infrastruktur inkl. der daran betriebenen IT-Systeme der Universität.

§ 3
Beteiligte am IT-Sicherheitsprozess

Im Sinn dieser Ordnung sind am IT-Sicherheitsprozess der Technischen Universität verantwortlich beteiligt:
- Der zentrale IT-Sicherheitsbeauftragte
- Dezentrale IT-Sicherheitsbeauftragte
- Der Sicherheitsstab
- Das Rechenzentrum der TU
- Alle Einrichtungen der Technischen Universität

§ 4
IT-Sicherheitsbeauftragte

(1) Die Hochschulleitung bestellt einen zentralen IT-Sicherheitsbeauftragten und einen Stellvertreter.

(2) Jeder Fachbereich, jede zentrale Einrichtung sowie die Verwaltung hat einen IT-Sicherheitsbeauftragten und Stellvertreter zu benennen (dezentraler Sicherheitsbeauftragter). Mehrere Fachbereiche können einen gemeinsamen Sicherheitsbeauftragten benennen.

Durch diese Benennungen müssen alle IT-Systeme im Geltungsbereich sowie die vor Ort für deren Betrieb verantwortlichen Personen einem IT-Sicherheitsbeauftragten auf Fachbereichs- oder Einrichtungsebene zugeordnet sein.

(3) Bei der Bestellung/Benennung der IT-Sicherheitsbeauftragten sollen der strategische Aspekt und die dafür erforderliche personelle Kontinuität berücksichtigt werden. Die IT-Sicherheitsbeauftragten sollen deshalb möglichst zum hauptamtlichen Personal der Universität gehören. Sie sollen in IT-Sicherheitsfragen besonders geschult werden.

§ 5
Sicherheitsstab

(1) Ständige Mitglieder des Sicherheitsstabs sind:
- der zentrale IT-Sicherheitsbeauftragte (Vorsitz)
- ein Vertreter des Rechenzentrums
- ein Vertreter des Rechtsdezernats
- der Datenschutzbeauftragte der Technischen Universität

(2) Der Gesamtpersonalrat kann ein beratendes Mitglied benennen.

(3) Weitere IT-sachverständige Mitglieder werden von der Hochschulleitung benannt. Die Anzahl der Mitglieder des Sicherheitsstabes soll 10 nicht überschreiten.

§ 6
Aufgaben der Beteiligten

(1) Der zentrale IT-Sicherheitsbeauftragte ist für Konzeption, Umsetzung und Überwachung des IT-Sicherheitsprozesses verantwortlich.

(2) Das Rechenzentrum ist verantwortlich für die system-, netz- und betriebstechnischen Aspekte der IT-Sicherheit und gibt in diesem Rahmen Empfehlungen zu technischen Standards zur IT-Sicherheit für die TU vor.

(3) Der Sicherheitsstab unterstützt den zentralen IT-Sicherheitsbeauftragten, indem er Pläne, Leitlinien und Vorgaben für sämtliche übergreifenden Belange der IT-Sicherheit erarbeitet, Maßnahmen koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.

(4) Die dezentralen IT-Sicherheitsbeauftragten sind für alle Sicherheitsbelange der IT-Systeme und -Anwendungen in den Bereichen, die ihnen jeweils zugeordnet sind, verantwortlich. Dabei haben sie die Vorgaben des Sicherheitsstabes zu beachten.

(5) Die Einsetzung von IT-Sicherheitsbeauftragten entbindet die Leitungen der Einrichtungen nicht von ihrer Verantwortung zur Umsetzung der IT-Sicherheit in ihrem Bereich.

(6) Die Einrichtungen der Technischen Universität sind verpflichtet, bei allen Planungen, Verfahren und Entscheidungen mit Bezug zur IT-Sicherheit die jeweils zuständigen dezentralen IT-Sicherheitsbeauftragten zu beteiligen. Der dezentrale IT-Sicherheitsbeauftragte hat gegebenenfalls bei Entscheidungen den zentralen IT-Sicherheitsbeauftragten einzubeziehen.

§ 7
Der IT-Sicherheitsprozess

(1) Der zentrale IT-Sicherheitsbeauftragte initiiert, steuert und kontrolliert unter Beteiligung des Sicherheitsstabs den IT-Sicherheitsprozess, der nach festzulegenden Prioritäten Maßnahmen insbesondere zu schneller Krisenintervention umfassen muss. Zwecks Gewährleistung einer kontinuierlichen Steuerung des IT-Sicherheitsprozesses soll der Sicherheitsstab regelmäßig tagen.

(2) Die dezentralen IT-Sicherheitsbeauftragten sind verpflichtet, sicherheitsrelevante Informationen jederzeit entgegenzunehmen und das jeweils Erforderliche zu veranlassen. Soweit notwendig, informieren sich dezentrale IT-Sicherheitsbeauftragte zu Ursachen und Maßnahmen durch Kontaktaufnahme zum zentralen IT-Sicherheitsbeauftragten und/oder zum Rechenzentrum.

(3) Die dezentralen IT-Sicherheitsbeauftragten sind für die kontinuierliche Überwachung der Umsetzung des IT-Sicherheitsprozesses in ihrem Bereich verantwortlich. Sie informieren sich regelmäßig über die Sicherheit der IT-Systeme in ihrem Bereich und veranlassen unverzüglich die notwendigen Maßnahmen zur Gewährleistung der erforderlichen Sicherheit. Sie informieren die Leitung ihrer Einrichtung regelmäßig über den Sicherheitsstandard und auftretende Probleme und schlagen Lösungsmöglichkeiten vor.

(4) Der zentrale IT-Sicherheitsbeauftragte berichtet der Hochschulleitung und dem Senat aus gegebenem Anlass darüber und macht Vorschläge für die Weiterentwicklung des IT-Sicherheitsprozesses unter Berücksichtigung der Ausgewogenheit, Durchgängigkeit und Angemessenheit der Maßnahmen. Dabei ist die Höhe der voraussichtlichen Kosten der einzelnen Maßnahmen anzugeben.

(5) Die dezentralen IT-Sicherheitsbeauftragten sind bezüglich ihrer Mitteilungspflichten gegenüber dem zentralen IT-Sicherheitsbeauftragten, der Hochschulleitung und dem Senat unabhängig von Weisungen ihrer Vorgesetzten. Die IT-Sicherheitsbeauftragten geben ihre Berichte auch den Leitungen der betreffenden Einrichtungen zur Kenntnis.

§ 8
Gefahrenintervention

(1) Bei Gefahr in Verzug veranlassen die dezentralen IT-Sicherheitsbeauftragten die sofortige vorübergehende Stilllegung betroffener IT-Systeme in ihrem Bereich, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden - insbesondere für andere Einrichtungen oder für die IT-Infrastruktur der Technischen Universität in Teilen oder insgesamt - nicht anders abzuwenden ist. Unverzüglich sind die Leitung der Einrichtung und das Rechenzentrum zu benachrichtigen, das seinerseits den zentrale/n IT-Sicherheitsbeauftragten benachrichtigt.

(2) Soweit das Rechenzentrum Gefahr in Verzug feststellt, kann es Netzanschlüsse (ggfs. auch ohne vorherige Benachrichtigung der Betroffenen) vorübergehend sperren, wenn zu befürchten ist, dass ein voraussichtlich gravierender Schaden für die IT-Infrastruktur der Technischen Universität in Teilen oder insgesamt nicht anders abzuwenden ist. Die Benachrichtigung des zuständigen dezentralen sowie des zentralen IT-Sicherheitsbeauftragten erfolgt unverzüglich ggfs. nachträglich.

(3) Vor Wiederinbetriebnahme vorübergehend stillgelegter Systeme bzw. gesperrter Netzanschlüsse ist in der Regel die Durchführung hinreichender Sicherheitsmaßnahmen erforderlich. Im Zweifelsfall entscheidet der zentrale IT-Sicherheitsbeauftragte über das weitere Vorgehen.

§ 9
Finanzierung

(1) Die Mittel für spezielle, mit dem zentralen IT-Sicherheitsbeauftragten und dem Rechenzentrum abgestimmte Sicherheitsmaßnahmen in den Einrichtungen der Technischen Universität sowie insbesondere Mittel zur Schulung für die dezentralen IT-Sicherheitsbeauftragten sind von den betreffenden Einrichtungen aufzubringen, die Mittel für diese Zwecke in ihrer Finanzplanung angemessen zu berücksichtigen haben.

(2) Soweit Sicherheitsmaßnahmen aus zentralen Mitteln finanziert werden müssen, ordnet der zentrale IT-Sicherheitsbeauftragte in Abstimmung mit dem Sicherheitsstab diese nach Dringlichkeit in einer Liste. Mit einer Begründung der Prioritäten schlägt er der Hochschulleitung die Finanzierung vor.

§ 10
Inkrafttreten

Diese Ordnung tritt am Tag nach ihrer hochschulöffentlichen Bekanntmachung in Kraft.